

# Access Control System over Internet

Santhoshkumar G.S

*Associate Professor, Department of Computer Science  
Amal Jyothi College of Engineering, Kottayam, 686518, Kerala, India*

Sweety Wilson

*Department of Computer Science  
Amal Jyothi College of Engineering, Kottayam, 686518, Kerala, India*

Ligimol Varghese

*Department of Computer Science  
Amal Jyothi College of Engineering, Kottayam, 686518, Kerala, India*

**Abstract-** In every organization security is an area where utmost significance must be given. Besides providing protection to employees who are working, there must be a proper way of authorizing who has the access to enter into important areas. Unlawful entry of any employee can cause severe damage to the organization. An access control system distinguishes personnel with authorized access from unauthorized individual. The system does this authorization using smart cards integrated with the technology of radio frequency identification (RFID). Smart card will be issued to employees with a unique card serial number (CSN) stored in it. A transfer of energy between smart card of employee and card reader takes place through contactless near field communication. The system combines RFID technology and Arduino IDE to accomplish the required task. The authorization using access control system is done in the following manner the CSN is read and is checked with stored data. If card is under unblocked category the employee has to verify himself/herself by fingerprint. Based on this two-factor authentication access is granted otherwise it is denied. Thus, it provides flexible control over who is allowed to enter premises of an organization.

**Keywords – RFID and Finger Print Based Dual Security System, MFRC522, ESP8266, R307 Module, CSN**

## I. INTRODUCTION

Access control systems are the electronic systems that are designed to control through a network and they should have an access to a network. It recognizes authenticates and authorizes entry of a person to enter into the premise thereby giving complete protection ensuring security with the system. In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource while access management describes the process. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. An authentication factor is a piece of information and process used to authenticate a person's identity for security purposes.

Two-factor authentication (2FA) is an authentication mechanism based on two pieces of information: something you have, such as a smart card, token id, etc. and something you know, such as a PIN. When presented with a log-on option, the user must provide both pieces of the authentication mechanism or they will be denied access to the system. There is another factor of authentication providing multifactor authentication based on something a person is or does, such as a biometric recognition. Hence a combined solution using RFID and smartcard-based biometrics like finger print can enhance the security and performance of an access control system which overcome flaws of traditional access control.

## II. PROPOSED ALGORITHM

### 2.1 The Embedded System –

The project aims at the authorized persons into the area and it will not allow the unauthorized persons and it displays that whether access is permitted or not. The embedded system consisting of Arduino Uno which act as a microprocessor. Detail of smart cards are read using MFRC522 Reader. RFID technology is used these contactless smart cards. The unique Card Serial Number (CSN) is matched against the one stored in database. If a match is

found it checks whether card belong to is blocked attribute. If it is not employee verifies his/her fingerprint against the stored one. A relay switch is used to control on or off of electrical bulb. Glowing of electrical bulb symbolize opening of door or turnstile indicates that the person is authorized. Thus, it keeps unauthorized personnel from accessing crucial areas of an organization.

RFID Smart Cards store information on a chip embedded in the smart card. The chip contains an embedded secure microprocessor or equivalent intelligence and internal memory. An antenna is also embedded in the plastic body of the card. RFID induction technology is used for communication between the card and the reader and also powers the card. The RFID technology used in this case works over a short range of fewer than 4 inches. As such, the card should be held near to the reader. Both the card and the reader communicate using radio frequencies via their embedded antennae. Following is a summary of the sequence of events that take place when the card is brought near the reader.

- Energy is transferred to the card that powers the chip inside the card
- Clock signals are transferred from reader to card
- Data transferred from reader to card
- Data transferred from card to reader

## 2.2. Components of Access Control System –

Arduino Uno: Arduino Uno is a microcontroller board. To this board fingerprint module, keypad and relay are connected.



Figure 2.2.1: Arduino Uno

Wi-Fi Module: Wi-Fi module named ESP 8266 is used to connect to network and RFID reader is attached to it.



Figure 2.2.2: ESP8266 Wi-Fi module

RFID Reader: MRC522 is used to read and write the details of smart cards with embedded chips. The working frequency is 13.56MHz.



Figure 2.2.3: MRC522

Smart Card: A chip is embedded inside the smart card or key fob, which responds to RFID reader through power transfer.



Figure 2.2.4: Smart card and key fob

Fingerprint Sensor Module: For reading the fingerprint, R307 Fingerprint Reader Sensor Module is used. It uses optical technology to precisely capture fingerprint.



Figure 2.2.5: Fingerprint sensor

Keypad: A hex 4x4 keypad is used to enter PIN information and is attached to microcontroller.



Figure 2.2.6: Keypad

Relay Driver: Relay is used to turn on and off the electrical bulb.



Figure 2.2.7: Relay

Electrical Bulb: When employee's access is verified as authorized the relay is turned on. As a result, LED bulb which simulates as a lock glows for few seconds.



Figure 2.2.8: Bulb

## 2.2 Working of Access Control System –

The concept of access control using Arduino & RFID technology is that to control the Door automatically. In this method RFID reader Arduino board is placed far away to the door, whenever person (he/she is having RFID smart card) comes nearer to the Reader, RFID reader reads the data from his RFID tag. This data is sent to the Arduino board, which is basically Microcontroller based board. Arduino board receives that card CSN and compares with valid numbers.

If the CSN (Card Serial Number) is among the blocked list access is denied otherwise when a match is found fingerprint of the user is read. The fingerprint is verified against the stored one and access is permitted and if match is not found the user can give a secret PIN known to him. If it is a matching PIN with that stored in database access provided otherwise access is denied.

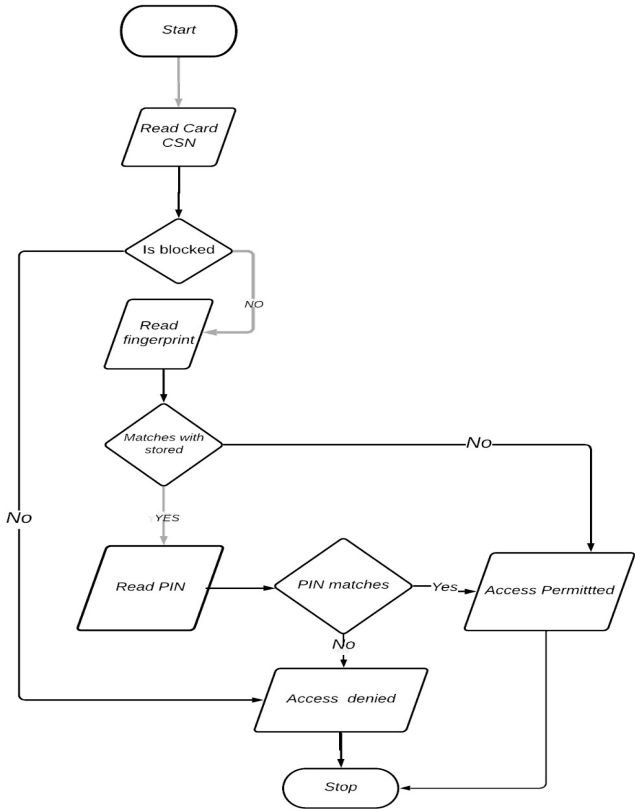


Figure 2.3.1: Flowchart of Access Control System

III. EXPERIMENT AND RESULT

3.1 The Embedded System –

The Figure 3.1.1 shows an arrangement of the embedded system which consists of a micro-controller Arduino Uno, Rc522 card reader, ESP8266 Wi-Fi module a fingerprint sensor, a relay driver and a LED bulb. A smart card is placed over the RC522 reader.

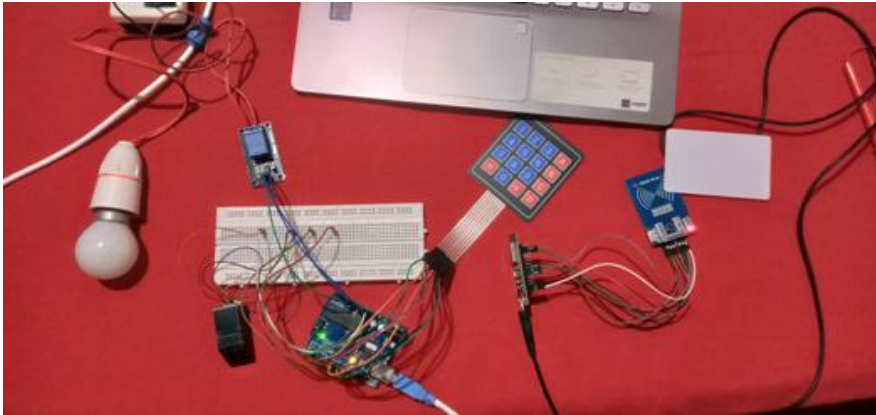


Figure 3.1.1: Circuit diagram of Access control System

3.2 Database details –

Figure 3.2.1 shows the database contents which contains attributes related to an employee. This made with MariaDB of XAMPP software.

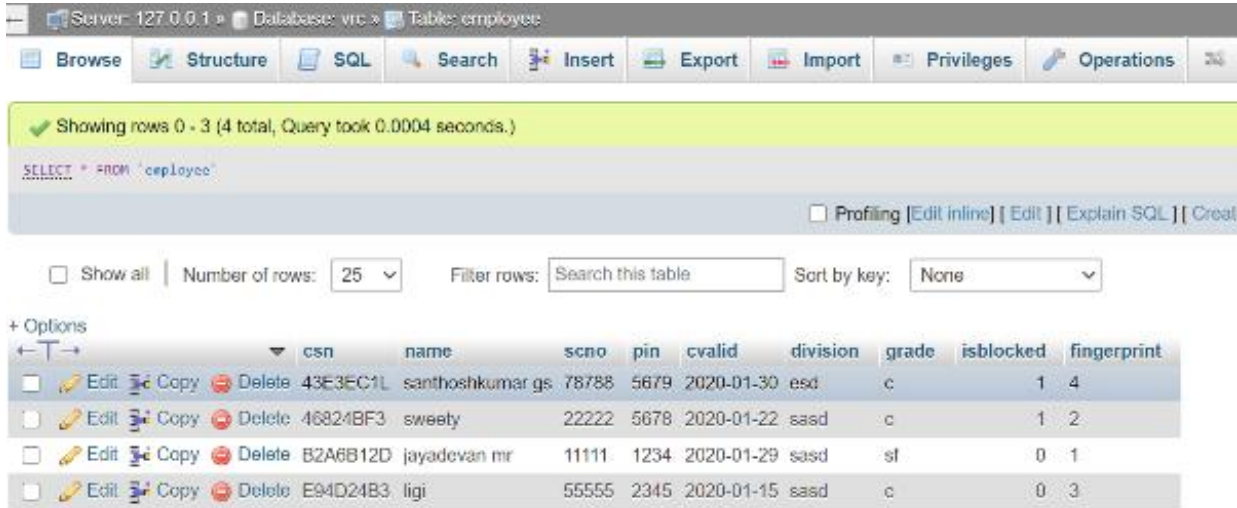


Figure 3.2.1: Details of Employee in database

3.3 Serial monitor Output when card is read –

Figure 3.3.1 shows the output in serial monitor of Arduino when card details are checked.



Figure 3.3.1: Output when card details are being verified

### 3.4 Authorized Access –

Figure 4.5 shows relay has turned the circuit connecting the LED bulb into operating condition. An authorized access permitted to an employee is indicated by glowing of bulb for few seconds. Bulb is used as a prototype of solenoid locks in actual scenario of doors and turnstiles.

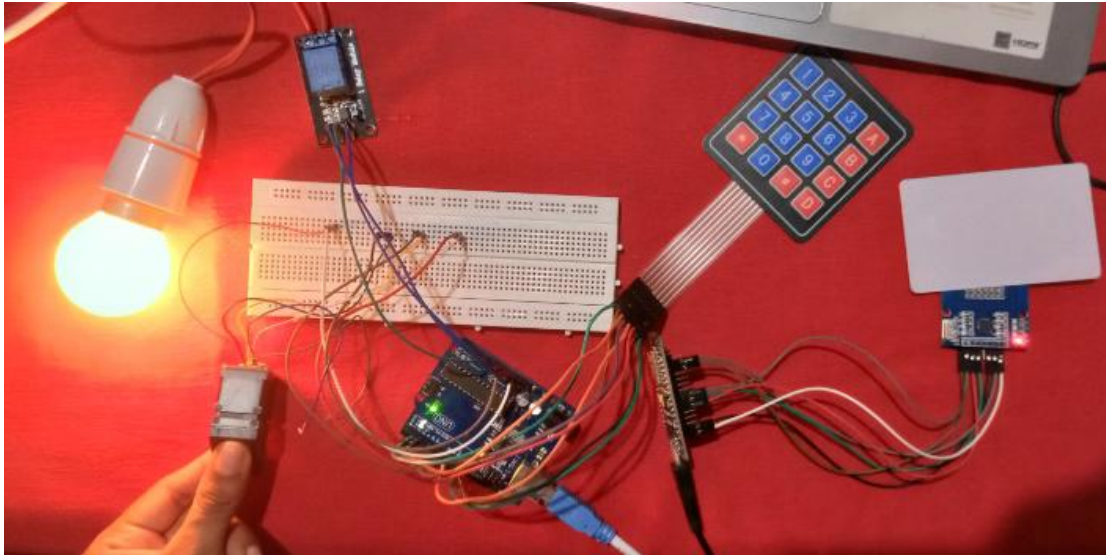


Figure 3.4.1: When authorized access happens

## IV. CONCLUSION

The access to a restricted area is normally done through a manual system of keys and locks. In our proposed system we make use of smart cards using RFID technology along with verification of users fingerprint. The sensor and fingerprint processor is integrated with an RFID technology smart card. The smart card will store the fingerprint of the authorized user. When the card is used and the authentication is successful; the RFID circuit is enabled to transmit data to the RFID reader which reads the information transmitted and allow access to the user if he is authenticated otherwise entry is restricted.

The added biometrics verification with smart card offers high level identification management security operations that have several advantages over traditional means and our system is very quicker and reliable.

## REFERENCES

- [1] Sercan AYGUN, "Smart Card And Biometric Based General Purpose Access Control System Design," ResearchGate June 2015.
- [2] Tarang Chugh, Kai Cao, and Anil K. Jain: "Fingerprint Spoof Buster: Use of Minutiae-centered Patches." IEEE March 2018.
- [3] Nesar Ali et al: "RFID and Finger Print Based Dual Security System: A Robust Secured Control to Access Through Door Lock Operation." American Journal of Embedded Systems and Applications June 15, 2018.
- [4] Hitesh Walia, Neelu Jain: "Fingerprint Based Attendance Systems-A Re-view." International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September 2016.
- [5] J. Baidya, T. Saha, R. Moyashir and R. Palit: "Design and implementation of a fingerprint based lock system for shared access," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448.
- [6] E. Ngai and F. Riggins, "RFID: Technology applications and impact on business operations" in International Journal of Production Economics, Elsevier, vol. 112, no. 2, pp. 507-509, 2008.
- [7] Consuela Simukali, Jackson Phiri, Stephen Namukolo, "Multi Factor Authentication for Student and Staff Access Control." (IJACSA) International Journal of Advanced Computer Science and Applications, 2019
- [8] V. V. Annarita Drago, "Methods and Techniques for Enhancing Physical Security of Critical Infrastructures Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione," March 2015
- [9] Jebah Jaykumar, Abishlin Blessy, "Secure Smart Environment Using IOT based on RFID." (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 2493-2496